Document View

« Back to Results

< Previous Document 7 of 33 Next

Print | Email | Copy link | Cite this | Mark Document

Translate document from: Select language

Key security unlocked

Parker, Tim. **Canadian Computer Reseller**. Toronto: Aug 6, 1997.
Vol. 10, Iss. 15; pg. 42

Abstract (Summary)
After a series of break-ins to a large university computer, I was asked to look at protection mechanisms for e-mail being sent through the system. While the usual approach for protecting such data is encryption, I was surprised to learn that few of the administrators knew very much about the subject. Public-private key encryption -- which bypasses the problem of having to send the password to the recipient -- was a virtually unknown topic among the people I dealt with. Assuming that readers, too, may be unfamiliar with this technology, here's a quick look at the use of digital signatures and public-private key encryption. Standard encryption uses a password to convert a readable file to one filled with seemingly random bytes, making it unreadable until the same password is used to convert the file back to readable format. To decrypt the file, you need the encrypting password, which must somehow be sent to the file's recipient. That leaves the password open to interception, and the file can then be decrypted. Public key encryption relies on two passwords for each user: the private key, which is kept secret by the user; and, the public key, which is made available to anyone who wants it (such as through a Web page).When I want to send a file to someone, I get their public key and use it to encrypt the file. The file can then he sent through unsecure channels to the recipient, who uses a private key to decrypt the message.

» Jump to indexing (document details)

Full Text (801 words)

After a series of break-ins to a large university computer, I was asked to look at protection mechanisms for e-mail being sent through the system. While the usual approach for protecting such data is encryption, I was surprised to learn that few of the administrators knew very much about the subject. Public-private key encryption -- which bypasses the problem of having to send the password to the recipient -- was a virtually unknown topic among the people I dealt with. Assuming that readers, too, may be unfamiliar with this technology, here's a quick look at the use of digital signatures and public-private key encryption. Standard encryption uses a password to convert a readable file to one filled with seemingly random bytes, making it unreadable until the same password is used to convert the file back to readable format. To decrypt the file, you need the encrypting password, which must somehow be sent to the file's recipient. That leaves the password open to interception, and the file can then be decrypted. Public key encryption relies on two passwords for each

user: the private key, which is kept secret by the user; and, the public key, which is made available to anyone who wants it (such as through a Web page).When I want to send a file to someone, I get their public key and use it to encrypt the file. The file can then he sent through unsecure channels to the recipient, who uses a private key to decrypt the message. Obviously, there is a relationship between each user's public and private key, but it's a complex mathematical formula that guarantees that only the owner of the private key can decrypt files. If someone was able to intercept the encrypted file I sent, and they had the recipient's public key, they wouldn't be able to decrypt the file. Only the private key can decrypt a file. This may sound rather complex, but it's not. There are many public key systems on the market, some commercial and some readily available to anyone, such as Pretty Good Privacy (PGP), which is free. To use the public key software, you provide a password to a utility that generates a public key "signature," which you can attach to your e-mail messages. Anyone who receives your public key can use it to encrypt messages specifically for you. When an encrypted message arrives, you supply your password or the location of the private key, and the message is decrypted. The entire process can be reduced to a drag-and-drop operation on most systems, so user overhead is minimal. How secure is public key technology? So far it has proven to be excellent. Although it's possible to break the encryption method, it requires computer horsepower far beyond what most of us have access to. It's so good, in fact, that the U.S. government tried to restrict the author of PGP from distributing his software, arguing it made it difficult for government agencies to monitor the population. An additional benefit to public key systems is the use of digital signatures. This is another key used to "sign" something that you're sending out. When the recipient gets the file, their utilities can verify that it was indeed you who sent the file. Digital signatures are a sure-fire method of ensuring that you know who is sending you material, and proving that files came from you. Finally, a quick update on one of my earlier Java columns. As most readers know, ⓘSun Microsystems, which owns and licenses Java, has been pushing Java since it was developed two years ago. To try and keep the development language in the forefront, it has announced a few new Java developments. First, Sun has launched the Personal Java Application Programming Interface (API), which is aimed at devices such as the network computer and TV-based Web systems. The Personal Java API is intended to allow manufacturers to use **Java** for a variety of purposes, but so far only **WebTV** Networks has signed up. ⓘSun's new Embedded **Java** API is a similar programming tool designed to run on low-horsepower CPUs such as those in telephones and fax machines. A number of companies are signing up for this API, but no products incorporating Java have been announced yet. ⓘSun has also announced the Java Card standard, which is designed to provide Java-based "smart cards," such as pre-paid bank debit cards and telephone cards. Although the two largest manufacturers of smart cards -- Gem-plus and ⓘSchlumberger -- are Java licencees, there's no word on what's going to happen with the Java Card standard. Still, it's nice to see ⓘSun pushing Java and trying to make it more widely available. I just wonder when all this wonderful Java-based wizardry we've been hearing about for two years is going to come to fruition.

Indexing (document details)

Subjects:	Computer files, Security measures, Data encryption
Classification Codes	9172 Canada
Author(s):	Parker, Tim
Publication title:	Canadian Computer Reseller. Toronto: Aug 6, 1997. Vol. 10, Iss. 15; pg. 42
Source type:	Periodical
ISSN:	08407312

ProQuest document ID: 418335921

Text Word Count 801

Document URL: http://proquest.umi.com/pqdweb?did=418335921&sid=1&Fmt=7&clientId=19649&RQT=309&VName=PQD

[File 344] **Chinese Patents Abs** Jan 1985-2006/Jan

**File 344: This file is no longer updating. For comprehensive coverage of Chinese patents, please use INPADOC, File 345.*

[File 348] **EUROPEAN PATENTS** 1978-2007/ 200744

**File 348: For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.*

[File 349] **PCT FULLTEXT** 1979-2007/UB=20071108UT=20071101

**File 349: For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.*

```
?
?  s ((set(n1) top(n1)box) or PCTV or webtv)(n16(shopping(n1)(cart or
basket))
>>>W:  Invalid syntax
>>>E:  There is no result

?  s ((set(n1)top(n1)box) or PCTV or webtv)(n16)(shopping(n1)(cart or
basket))
Processing
Processing
Processing
Processing
Processing
     21551297   SET
     16761916   TOP
      4244132   BOX
       128693   SET(1N)TOP(1N)BOX
         3497   PCTV
        29336   WEBTV
      3466136   SHOPPING
       266469   CART
       498180   BASKET
S1          2   S ((SET(N1)TOP(N1)BOX) OR PCTV OR
WEBTV)(N16)(SHOPPING(N1)(CART OR BASKET))
```

```
?  s ((SET(N1)TOP(N1)BOX) OR PCTV OR WEBTV)(N16)(order or purchase)
Processing
Processing
Processing
Processing
Processing
Processing
     21551297   SET
     16761916   TOP
      4244132   BOX
       128693   SET(1N)TOP(1N)BOX
         3497   PCTV
        29336   WEBTV
     16247777   ORDER
      6458691   PURCHASE
S2       5326   S ((SET(N1)TOP(N1)BOX) OR PCTV OR WEBTV)(N16)(ORDER OR
PURCHASE)

?
?  s s2 and pd<19970912
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
Processing
>>>W:  One or more prefixes are unsupported
  or undefined in one or more files.
         5326   S2
     53039888   PD<19970912
S3        815   S S2 AND PD<19970912

?  s s3 and shopping
          815   S3
      3466136   SHOPPING
S4        125   S S3 AND SHOPPING
```

EFF KWJC
11/18/07

Recent Searches

Close window | Help

Add terms to your search using: AND

3. ((shopping w/1 cart) w/10 tvml) AND PDN(<9/12/1997) — 0 result — Add to Search
   Database: Multiple databases...
   Look for terms in: Citation and document text
   Publication type: All publication types
   Set Up Alert
2. ((shopping w/1 cart) w/10 java) AND PDN(<9/12/1997) — 12 results — Add to Search
   Database: Multiple databases...
   Look for terms in: Citation and document text
   Publication type: All publication types
   Set Up Alert
1. (webtv w/10 java) AND PDN(<9/12/1997) — 33 results — Add to Search
   Database: Multiple databases...
   Look for terms in: Citation and document text
   Publication type: All publication types
   Set Up Alert

Close window | Help